What is claimed is:

1. A method for detecting least significant bit ("LSB") embedding of a message hidden in randomly scattered samples of an alleged cover image, comprising the steps of:

dividing the alleged cover image into a plurality of disjoint groups of adjacent samples;

defining a discrimination function that assigns a real number to each member of said plurality, thereby capturing the smoothness of each of said groups;

defining on said plurality at least one invertible operation that comprises a permutation of sample values, whereby values of said samples are invertibly perturbed by a small amount;

applying said discrimination function and said ~~flipping operation~~ to define in said plurality three types of sample groups, (R)egular , (S)ingular, and (U)nusable, each of said types being defined for both positive and negative operations;

plotting both positive and negative R and S for said alleged cover image on an RS diagram;

constructing four curves of said RS diagram and calculating their intersections by extrapolation; and

determining the existence or nonexistence of a secret message from said intersections.

2. The method of claim 1, further including the step, if said secret message is determined to exist, of estimating a length thereof.

3. The method of claim 2, wherein each of said samples is a pixel value.

4. The method of claim 3, wherein said pixel value is a grayscale.

5. The method of claim 3, wherein said pixel value is a color.

6. The method of claim 2, wherein each of said samples is an index to a palette of color values.

7. The method of claim 1, wherein said step of constructing further comprises arithmetically averaging the x coordinates of said intersections, thereby detecting said hidden message, if it exists, and estimating a length thereof.

8. The method of claim 2, wherein said step of estimating further comprises determining a length p of said hidden message, if it exists, by rescaling the x-axis of said RS diagram so that $p/2$ becomes 0 and $100 - p/2$ becomes 1, whereby an x-coordinate of an intersection is a root of the following quadratic equation:

$$2(d_1 + d_0)x^2 + (d_{-0} - d_{-1} - d_1 - 3d_0)x + d_0 - d_{-0} = 0,$$

where $d_0 = R_M(p/2) - S_M(p/2)$, $d_1 = R_M(1 - p/2) - S_M(1 - p/2)$, $d_{-0} = R_{-M}(p/2) - S_{-M}(p/2)$, $d_{-1} = R_{-M}(1 - p/2) - S_{-M}(1 - p/2)$, and said message length p is calculated from the root x whose absolute value is smaller,

$$p = x/(x-1/2).$$

9. Apparatus for detecting least significant bit ("LSB") embedding of a message hidden in randomly scattered samples of an alleged cover image, which comprises:

means for dividing said alleged cover image into a plurality of disjoint groups of adjacent samples;

first means for defining effective for defining a discrimination function that assigns a real number to each member of said plurality of disjoint groups, thereby capturing the smoothness of each of said groups;

second means for defining effective for defining on said plurality of disjoint groups at least one invertible operation that comprises a permutation of sample values, whereby values of said samples are invertibly perturbed by a small amount;

means for applying said discrimination function and said ~~flipping operation~~ invertible operation to define in said plurality three types of sample groups, (R)egular , (S)ingular, and (U)nusable, each of said types being defined for both positive and negative operations;

means for plotting both positive and negative R and S for said alleged cover image on an RS diagram;

means for constructing four curves of said RS diagram;

means for calculating the intersections of said four curves by extrapolation; and

first means for determining effective for determining from said intersections the existence or nonexistence of a secret message.

10. The apparatus of claim 9, further including means for estimating a length of said secret message if said secret message is determined to exist.

11. The apparatus of claim 10, wherein each of said samples is a pixel value.

12. The apparatus of claim 11, wherein said pixel value is a grayscale.

13. The apparatus of claim 11, wherein said pixel value is a color.

14. The apparatus of claim 10, wherein each of said samples is an index to a palette of color values.

15. The apparatus of claim 9, wherein said means for constructing and calculating is further effective for arithmetically averaging the x coordinates of said intersections, thereby detecting said hidden message and estimating a length thereof.

16. The apparatus of claim 10, wherein said means for estimating is effective for determining a length p of said hidden message by rescaling the x-axis of said RS diagram so that $p/2$ becomes 0 and $100 - p/2$ becomes 1, whereby an x-coordinate of an intersection is a root of the following quadratic equation:

$$2(d_1 + d_0)x^2 + (d_{-0} - d_{-1} - d_1 - 3d_0)x + d_0 - d_{-0} = 0,$$

where $d_0 = R_M(p/2) - S_M(p/2)$, $d_1 = R_M(1 - p/2) - S_M(1 - p/2)$, $d_{-0} = R_{-M}(p/2) - S_{-M}(p/2)$, $d_{-1} = R_{-M}(1 - p/2) - S_{-M}(1 - p/2)$, and said message length p is calculated from the root x whose absolute value is smaller,

$$p = x/(x\text{-}1/2).$$

17. A computer-readable storage medium embodying program instructions for a method for detecting least significant bit ("LSB") embedding of a message hidden in randomly scattered samples of an alleged cover image, said method comprising the steps of:

dividing said alleged cover image into a plurality of disjoint groups of adjacent samples;

defining a discrimination function that assigns a real number to each member of said plurality, thereby capturing the smoothness of each of said groups;

defining on said plurality at least one invertible operation that comprises a permutation of sample values, whereby values of said samples are invertibly perturbed by a small amount;

applying said discrimination function and said ~~flipping operation~~ to define in said plurality three types of sample groups, (R)egular , (S)ingular, and (U)nusable, each of said types being defined for both positive and negative operations;

plotting both positive and negative R and S for said alleged cover image on an RS diagram;

constructing four curves of said RS diagram and calculating their intersections by extrapolation; and

determining the existence or nonexistence of a secret message from said intersections.

18. The computer-readable storage medium of claim 17, said method further including the step, if said secret message is determined to exist, of estimating a length thereof.

19. The computer-readable storage medium of claim 17, said method further including, in said step of constructing, arithmetically averaging the x coordinates of said intersections, thereby detecting said hidden message, if it exists, and estimating a length thereof.

20. The computer-readable storage medium of claim 17, said method further including, in said step of estimating, determining a length p of said hidden message, if it exists, by rescaling the x-axis of said RS diagram so that $p/2$ becomes 0 and 100 - $p/2$ becomes 1, whereby an x-coordinate of an intersection is a root of the following quadratic equation:

$$2(d_1 + d_0)x^2 + (d_{-0} - d_{-1} - d_1 - 3d_0)x + d_0 - d_{-0} = 0,$$

where $d_0 = R_M(p/2) - S_M(p/2)$, $d_1 = R_M(1 - p/2) - S_M(1 - p/2)$, $d_{-0} = R_{-M}(p/2) - S_{-M}(p/2)$, $d_{-1} = R_{-M}(1 - p/2) - S_{-M}(1 - p/2)$, and said message length p is calculated from the root x whose absolute value is smaller,

$$p = x/(x\text{-}1/2).$$